Université Grenoble Alpes

Mails d'hameçonnage

Phishing emails

Comment les reconnaître ?

How to recognize them?

Procédure à destination des étudiants

Procedure for students

DGD SI - Université Grenoble Alpes
https://services-numeriques.univ-grenoble-alpes.fr
Assistance 04 56 52 97 20
sos-etudiants@univ-grenoble-alpes.fr

Table des matières – *Table of contents*

Introduction - *Introduction*

Parmi les nombreux courriels indésirables, certains sont plus pernicieux que d'autres puisqu'ils vont inciter le destinataire du message à divulguer des renseignements personnels dans le but de réaliser une usurpation d'identité. Ces messages d'hameçonnage, *phishing* en anglais, vont essayer de collecter directement ou en se faisant passer pour un tiers de confiance, des données personnelles telles qu'identifiant et mot de passe, coordonnées bancaires, etc.

Among the many spam emails some are more dangerous than others because they will try to steal personal information for example in order to impersonate you. This phishing emails will try to steal personal data like login, password or bank details, directly or pretending to be a trusted organization or person.

Cette technique d'ingénierie sociale, quand elle est diffusée par messagerie électronique, se base sur plusieurs éléments :

This social engineering technique when disseminated by email is based on several elements:

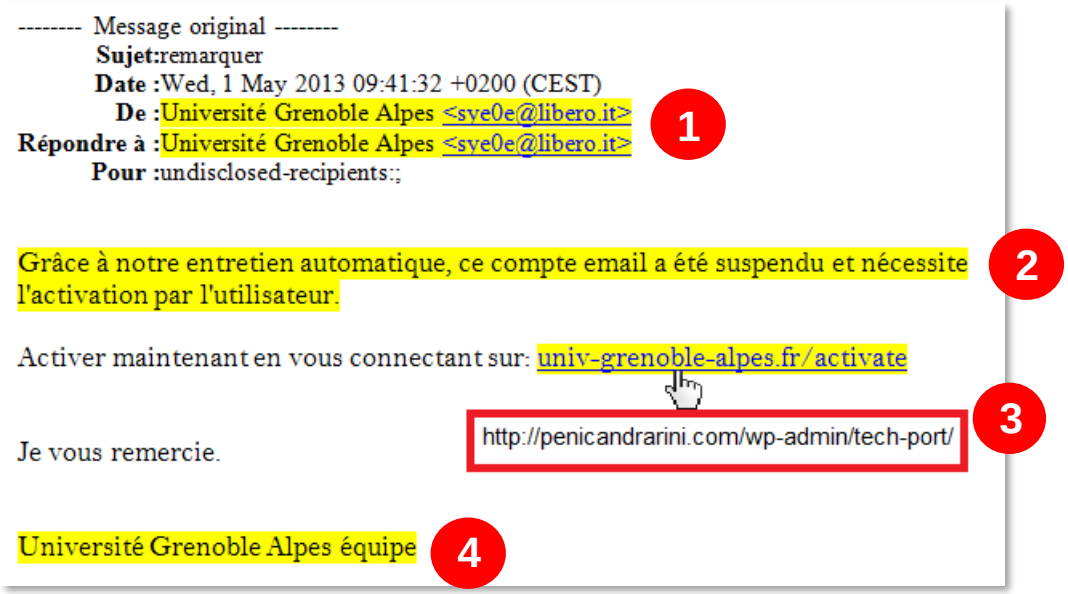
- elle va profiter de la lecture souvent trop rapide du message ;
  it will try to take advantage of the often too rapid reading of a message;

- elle va jouer sur une notion d'immédiateté de la réponse, sous peine de perdre un service ;
  it will use a notion of immediacy of the response on pain of losing a service;

- elle peut jouer sur la curiosité face à une catastrophe, ou un événement très médiatisé.
  it can use your curiosity about a disaster or a highly publicized event.

Comment les reconnaître ? – *How to recognize them?*

Exemple de message n°1 – *Example message #1*



Outre le fait que la DSI ne vous demandera jamais vos identifiants dans un message, voici ce qui devrait vous alerter pour reconnaître ou au moins suspecter un mail d'hameçonnage (*phishing*) :

Besides the fact that the IT department will never ask you for your login details in a message, here is what should alert you to recognize or at least suspect a phishing email:

1. Bien que l'adresse d'expéditeur soit aisément falsifiable, ici le fait qu'elle appartienne à un site italien (.it) et non au domaine univ-grenoble-alpes.fr doit nous alerter.

Although the sender's address is easily falsifiable, here the fact that it belongs to an Italian site (.it) and not to the univ-grenoble-alpes.fr domain should alert us.

2. Généralement, les *phishings* jouent beaucoup sur une immédiateté des décisions à prendre, pour éviter de perdre un service, et c'est le cas ici.

Generally, a phishing uses a lot the immediacy of the decisions you have to made, to avoid losing a service, and this is the case here.

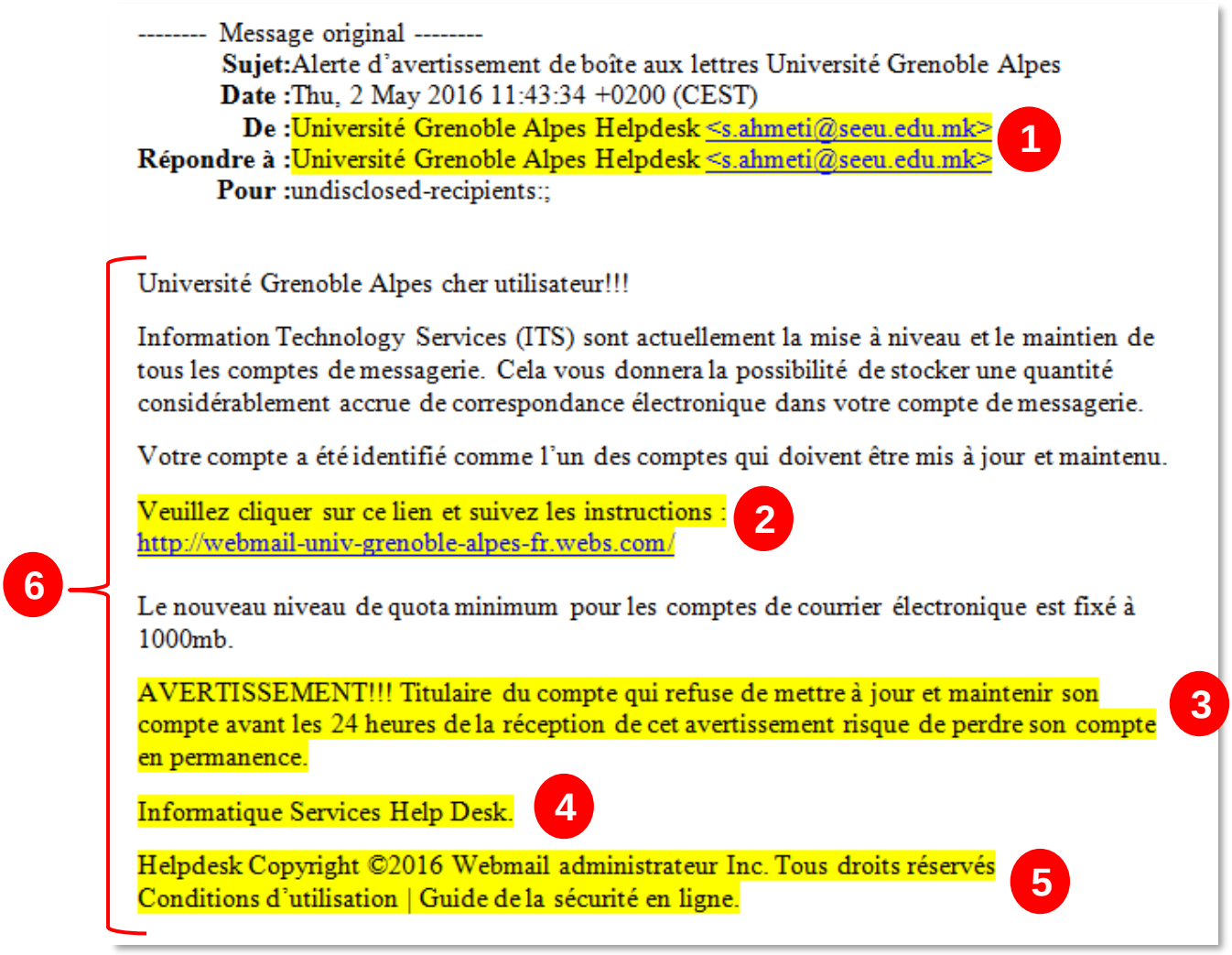
3. En **passant** la souris sur le lien, on voit s'afficher dans la barre de navigation (en bas de la page) la véritable adresse du lien : http://penicandrarini.com/wp-admin/tech-port/ qui, bien sûr, n'est pas un site de l'Université Grenoble Alpes.

By passing the mouse over the link, we see displayed in the navigation bar (at the bottom of the page) the real address of the link: http://penicandrarini.com/wp-admin/tech-port/ which is not a Université Grenoble Alpes website.

4. Une signature générique très vague, avec une tournure peu française, alors que les messages de la DSI sont généralement signés nominativement, avec l'adresse et le téléphone de la DSI.

A strange and too much generic signature, with an unusual structure, while the messages of the IT department are generally signed by name, with the address and the phone of the service.

Exemple de message n°2 – *Example message #2*



-------- Message original --------
Sujet: Alerte d'avertissement de boîte aux lettres Université Grenoble Alpes
Date : Thu, 2 May 2016 11:43:34 +0200 (CEST)
De : Université Grenoble Alpes Helpdesk <s.ahmeti@seeu.edu.mk> 1
Répondre à : Université Grenoble Alpes Helpdesk <s.ahmeti@seeu.edu.mk>
Pour :undisclosed-recipients:;

Université Grenoble Alpes cher utilisateur!!!

Information Technology Services (ITS) sont actuellement la mise à niveau et le maintien de tous les comptes de messagerie. Cela vous donnera la possibilité de stocker une quantité considérablement accrue de correspondance électronique dans votre compte de messagerie.

Votre compte a été identifié comme l'un des comptes qui doivent être mis à jour et maintenu.

Veuillez cliquer sur ce lien et suivez les instructions : 2
http://webmail-univ-grenoble-alpes-fr.webs.com/

Le nouveau niveau de quota minimum pour les comptes de courrier électronique est fixé à 1000mb.

AVERTISSEMENT!!! Titulaire du compte qui refuse de mettre à jour et maintenir son compte avant les 24 heures de la réception de cet avertissement risque de perdre son compte en permanence. 3

Informatique Services Help Desk. 4

Helpdesk Copyright ©2016 Webmail administrateur Inc. Tous droits réservés 5
Conditions d'utilisation | Guide de la sécurité en ligne.

6

1. La première partie du champ de l'expéditeur a été falsifiée (*Université Grenoble Alpes Helpdesk*), mais la seconde partie (s.ahmeti@seeu.edu.mk) renvoie à un domaine macédonien (.mk), et non au domaine univ-grenoble-alpes.fr. Cela doit nous alerter.

The first part of the sender's field has been falsified (Université Grenoble Alpes Helpdesk), but the second part (s.ahmeti@seeu.edu.mk) refers to a Macedonian domain (.mk), and not to the univ- grenoble-alpes.fr. This should alert us.

2. Le nom du lien doit nous alerter. Il contient bien « univ-grenoble-alpes.fr », mais est suffixé par quelque-chose d'étranger (ici **.webs.com**). Il ne renverra donc pas vers l'Université Grenoble Alpes.

*The name of the link should alert us. It does contain "univ-grenoble-alpes.fr", but is suffixed by something foreign (here **.webs.com**). It will not point at a Université Grenoble Alpes website.*

3. Généralement les *phishings* jouent beaucoup sur l'immédiateté d'une réponse à donner, pour éviter de perdre un service, et c'est le cas ici.

Generally, a phishing uses a lot the immediacy of the decisions you have to made, to avoid losing a service, and this is the case here.

4. Une signature générique très vague, alors que les messages de la DSI sont généralement signés nominativement, avec l'adresse et le téléphone de la DSI.

A too much generic signature, while the messages of the IT department are generally signed by name, with the address and the phone of the service.

5. Un copyright très étrange.

A very strange copyright.

6. Le texte est en français approximatif, sûrement issu d'un traducteur automatique.

The structure of the text is rough, certainly from an automatic translator.

Exemple de message n°3 – *Example message #3*

Il peut également vous arriver de recevoir un message d'un hacker vous informant qu'il vous surveille grâce à un cheval de Troie installé sur votre machine. Il prétend pouvoir vous en débarrasser moyennant une somme d'argent. Sachez que ce message n'est que de l'intimidation.

You may also receive a message from a hacker informing you that he's watching you by way of a Trojan horse installed on your computer. He claims he can get rid of it for a sum of money. Please be aware that this message is only intimidation.

Ces hackers obtiennent votre adresse de messagerie notamment grâce aux exemples de mail de *phishing* cités plus haut. En effet, si une personne clique sur un lien présent dans ce genre de message, cela permet aux hackers de récupérer les adresses mails de ses contacts, à qui ils enverront à leur tour des mails d'hameçonnage.

These hackers obtain your email address in particular thanks to the examples of phishing email mentioned above. Indeed, if a person clicks on a link present in this kind of message, this allows hackers to retrieve the email addresses of his contacts, to whom they will in turn send phishing emails.

Comment traiter ces messages ? – *How to treat these emails?*

1. Indiquer comme SPAM – *Treat as SPAM*

Dans votre messagerie, si ce n'est pas encore le cas, vous devez indiquer ce message comme étant un SPAM (courriel non désiré).

In your mailbox, if this isn't automatically the case, you must treat this message as a SPAM (junk mail).

2. Supprimer le message – *Delete the message*

Vous devez ensuite supprimer ce message définitivement dès réception (le supprimer également de votre corbeille et de votre dossier de spam).

You must then permanently delete this message upon receipt (also delete it from your trash and your junk mail folder).

3. Modifier votre mot de passe – *Change your password*

Si vous avez cliqué sur un lien dans un mail de phishing ou si vous recevez un message d'un hacker (exemple 3), il vous est fortement conseillé de modifier au plus vite votre mot de passe en suivant le lien ci-dessous :

https://copass-client.grenet.fr/app.php/simsu/secure/modifypwd/modify_password

Attention, le nouveau mot de passe ne sera actif que le lendemain de la modification.

If you clicked on a link in a phishing email or if you receive a message from a hacker (example 3), you are strongly advised to change your password as quickly as possible by following the link below:

https://copass-client.grenet.fr/app.php/simsu/secure/modifypwd/modify_password

Please note, the new password will not be active until the day after the modification.

4. Détecter les logiciels espions – *Detect spyware*

Certains logiciels espions échappent encore aux anti-virus.

L'outil « SpyBot - Search & Destroy » permet de les détecter et de les supprimer de votre machine.

Lancez SpyBot en mode avancé. Après l'analyse, vous pourrez sélectionner et supprimer les éventuels espions. En cas de mauvaise manipulation, il est possible de restaurer les programmes supprimés. SpyBot permet également de prévenir lors d'un éventuel téléchargement des espions sur Internet.

Plus d'informations et téléchargement sur le site de safer-networking.org

Some spyware still escapes anti-virus software.

The "SpyBot - Search & Destroy" tool allows you to detect and delete them from your computer.

Launch SpyBot in advanced mode. After the analysis, you will be able to select and delete any spies. In the event of deletion error, it's possible to restore the deleted programs. SpyBot also can to warn you the spyware downloads from the Internet.

More information and download on the safer-networking.org *website.*

5. Mettre à jour votre antivirus – *Update your antivirus*

S'il n'est pas à jour, récupérez les dernières données de votre anti-virus sur un poste qui n'est pas contaminé.

If it's not up to date, retrieve the antivirus latest data from a computer that isn't contaminated.